

目前课程内容已经完结，但依然在持续更新中。现在报名即赠送 Pixel2 手机一部，以及内部版本 FART12 自动化脱壳系统。更有 Frida 检测与绕过、定制版调试 ROM、内核定制等相关内容，马上报名，畅享丝滑体验！

课程优势

- 最底层的方案：从Art源码直击Java类和方法解释执行的根本原理
- 最前沿的工具：Fart重磅更新+船新脚本持久化框架FridaManager
- 最顶尖的技术：掌握一二代壳/DexVmp/Dex2C加固脱壳核心原理
- 最贴心的服务：超长两年服务时间/与大佬零距离亲密接触/纵享丝滑

- 五月：整体型壳的核心原理
 - 手写整体型壳：安卓动态加载机制,Classloader详解
 - Xposed脱壳插件：Xposed安装使用插件开发,FDexi详解
 - Frida脱壳脚本：Frida插件开发,DEXDump内存暴力脱壳
- 六月：打造整体脱壳沙箱
 - 安卓源码编译：源码版本/同步/编译,导入IDE阅读分析
 - App的加载流程：App生命周期,dexOoat流程分析脱壳
 - 寻找海量脱壳点：整体脱壳的本质,直接简介寻找脱壳点
- 八月：抽取型壳的核心原理
 - 壳的种类识别：壳与加固手段的甄别,手写反调试与绕过
 - 手写抽取型壳：Native GOT/PLT/inline hook详解与应用
 - 类加载和执行：Art中类加载和方法执行流程关键函数详解
- 九月：FART10，到来！
 - 构造主动调用：Art源码Review,Jni流程定制,方法体Dump
 - 方法体的回填：五元组格式解析,占坑型/偏移型的不同处理
 - Frida+Fart！：动态加载的Dex处理,单方法Dump,重构Fart！
- 十一月：DEX-VMP壳的核心原理
 - DEXVMP特征识别：App源码分析,特征识别,反编译二进流程分析
 - 手写DEXVMP壳：手写映射表,动态解密翻译执行Smali指令流
 - DEXVMP分析沙箱：Frida+沙箱动态追踪Vmp执行的Java方法
- 十二月：DEX-VMP分析与还原
 - 分析沙箱强化：强制解释模式,从Jni进行ArtMethod tracing
 - 搞定“拦路虎”：重编译内核&定制Art虚拟机绕过所有反调试
 - 重构映射表：HyperPwn直接调试Vmp分析重构原始映射表
- 二月：Dex2C的原理和分析
 - Jni&&反射：从Jni源码分析Java&C(++)互相调用完整流程
 - Dex2C加固应用：Dex2C加固流程,特征,执行和Frida动态分析
 - Dex2C逆向分析：定制解释执行分析沙箱,打造Jni四向tracer
- 三月：内部版FridaManager！
 - 原理与使用：使用环境和方法,原理和源码分析,插件编写详解
 - FridaGadgat：App启动过程和注入时机点选择,加载和Hook生
 - FridaManager：完全脱离PC,Fart移植,r0capture移植,制作沙箱

Fart脱壳王！从此没有脱不下来的壳！手把手教你打造陆地最强脱壳机
最新的工具和技巧，最实用和有效的方法，前人指路，一点即通；
高手带路，少走弯路，躺捡工具，节约时间，商务便捷，干净卫生；
同时希望营造一起研究、解决问题的环境，互惠互助、无缝交流；

FART脱壳王



长按扫码查看详情

- hanbingle
 - Fart全自动内存重组型脱壳机作者，开创Art脱壳新纪元
 - 资深移动安全专家，系统安全资深研究员
 - <https://bbs.pediy.com/user-home-632473.htm>
- roysue:
 - 喜欢和擅长 Frida，各种逆向经验丰富，老法师
 - FB, 极棒, 52pojie, 大会或各种场合演讲或分享，会棍
 - <https://github.com/r0ysue/AndroidSecurityStudy>
 - <https://www.anquanke.com/member/131652>

认真维护和分享技巧的知识星球

Fart脱壳王

微信扫码加入星球
知识星球



肉丝出品系列课程的特点和评价

- 果然跟着老师的操作来 是正确的，自己花里胡哨的 全报错。
- 碰上一个好师傅真的需要很好的运气
- 我是真的小白，进来之前啥都不会的，现在天天frida一把梭
- [强][强]肉丝大佬是学习逆向的指引者
- 入门门槛太高，小白自学太难了，没人带还真难搞--
- 越学才明显感觉到和肉丝师傅差距多大
- 安全的一下子跑到爬虫 就是一顿爆锤的赶脚
- 搞逆向必须要懂底层啊，这是趋势
- 5月的课直接让我完成了两个任务
- 被肉丝师傅带中，有个领路人确实走的比较快，比一个人瞎摸强
- 主要陈老师带的好，我也是看到混淆的类名，就用obj去搜名称 太稳了，把大家的思路培养出来了
- 其实没有陈老师指个方向 我现在还是无头苍蝇乱飞呢 [奸笑]我们只是在

该**自动化修复工具**专为报名学习 FART 脱壳王课程学员定制，针对赠送的 FART10 以及 FART12 脱壳获取的所有 dex 以及 bin 文件，可**自动化一键修复合并所有 dex 和 bin 文件**，不再需要一个一个进行修复。

具体使用流程如下：

1. 在使用 whitelist.txt 文件，完成要修复的类的主动调用后，直接 adb pull /sdcard/ooxx/packageName, 获取完整目录文件，该目录下有 FART10 以及 FART12 脱壳以及修复得到的所有 dex、txt、bin 文件，目录内容大致如下：

名称	修改日期	类型
9553800_dexfile_OpenCommon.dex	2023/11/20 23:01	DEX 文件
10480500_classlist_LoadMethod.txt	2023/11/20 23:01	文本文档
10480500_dexfile_LoadMethod.dex	2023/11/20 23:01	DEX 文件
10480500_dexfile_OpenCommon.dex	2023/11/20 23:01	DEX 文件
10545272_classlist_LoadMethod.txt	2023/11/20 23:01	文本文档
10545272_dexfile_LoadMethod.dex	2023/11/20 23:01	DEX 文件
10545272_dexfile_OpenCommon.dex	2023/11/20 23:01	DEX 文件
10978168_classlist.txt	2023/11/20 23:01	文本文档
10978168_classlist_LoadMethod.txt	2023/11/20 23:01	文本文档
10978168_dexfile.dex	2023/11/20 23:01	DEX 文件
10978168_dexfile_LoadMethod.dex	2023/11/20 23:01	DEX 文件
10978168_dexfile_OpenCommon.dex	2023/11/20 23:01	DEX 文件
10978168_ins_9461.bin	2023/11/20 23:01	BIN 文件
10978168_ins_9718.bin	2023/11/20 23:01	BIN 文件
10978168_ins_9803.bin	2023/11/20 23:01	BIN 文件

2. 启动 cmd，执行 java -jar repireall folderpath 即可开始对该目录下的所有 dex 和 bin 文件的合并修复，下图为开始修复截图，此时开始逐个对 dex 使用 bin 文件进行自动化修复。

```
C:\Users\tom\Desktop\FART脱壳王定制版自动化修复工具>java -jar repireall.jar test
Made By hanbingle for FART脱壳王课程，欢迎报名学习加固核心原理、脱壳攻防实战相关内容！微信搜索“大数据安全技术学习”公众号查看课程内容。
Start Repire all dexfile,Plase wait.....
start repire dexfile:C:\Users\tom\Desktop\FART脱壳王定制版自动化修复工具\test\10978168_dexfile.dex->with insfile:C:\Users\tom\Desktop\FART脱壳王定制版自动化修复工具\test\10978168_ins_9461.bin
repiredfolder->C:\Users\tom\Desktop\FART脱壳王定制版自动化修复工具\repire
success repire->C:\Users\tom\Desktop\FART脱壳王定制版自动化修复工具\repire\10978168_dexfile.dex_repired.dex
start repire dexfile:C:\Users\tom\Desktop\FART脱壳王定制版自动化修复工具\test\10978168_dexfile_LoadMethod.dex->with insfile:C:\Users\tom\Desktop\FART脱壳王定制版自动化修复工具\test\10978168_ins_9461.bin
repiredfolder->C:\Users\tom\Desktop\FART脱壳王定制版自动化修复工具\repire
success repire->C:\Users\tom\Desktop\FART脱壳王定制版自动化修复工具\repire\10978168_dexfile_LoadMethod.dex_repired.dex
start repire dexfile:C:\Users\tom\Desktop\FART脱壳王定制版自动化修复工具\test\10978168_dexfile_OpenCommon.dex->with insfile:C:\Users\tom\Desktop\FART脱壳王定制版自动化修复工具\test\10978168_ins_9461.bin
repiredfolder->C:\Users\tom\Desktop\FART脱壳王定制版自动化修复工具\repire
success repire->C:\Users\tom\Desktop\FART脱壳王定制版自动化修复工具\repire\10978168_dexfile_OpenCommon.dex_repired.dex
start repire dexfile:C:\Users\tom\Desktop\FART脱壳王定制版自动化修复工具\test\10978168_dexfile.dex->with insfile:C:\Users\tom\Desktop\FART脱壳王定制版自动化修复工具\test\10978168_ins_9718.bin
repiredfolder->C:\Users\tom\Desktop\FART脱壳王定制版自动化修复工具\repire
success repire->C:\Users\tom\Desktop\FART脱壳王定制版自动化修复工具\repire\10978168_dexfile.dex_repired.dex
Repire all dexfile end!Please enjoy!
```

3. 当修复完成后，此时会打印 Rrepire all dexfile end!提示，此时代表自动化修复已经结束。

```
start repire dexfile:C:\Users\tom\Desktop\FART脱壳王定制版自动化修复工具\test\10978168_dexfile_LoadMethod.dex->with insfile:C:\Users\tom\Desktop\FART脱壳王定制版自动化修复工具\test\10978168_ins_9803.bin
repiredfolder->C:\Users\tom\Desktop\FART脱壳王定制版自动化修复工具\repire
success repire->C:\Users\tom\Desktop\FART脱壳王定制版自动化修复工具\repire\10978168_dexfile_LoadMethod.dex_repired.dex
start repire dexfile:C:\Users\tom\Desktop\FART脱壳王定制版自动化修复工具\test\10978168_dexfile_OpenCommon.dex->with insfile:C:\Users\tom\Desktop\FART脱壳王定制版自动化修复工具\test\10978168_ins_9803.bin
repiredfolder->C:\Users\tom\Desktop\FART脱壳王定制版自动化修复工具\repire
success repire->C:\Users\tom\Desktop\FART脱壳王定制版自动化修复工具\repire\10978168_dexfile_OpenCommon.dex_repired.dex
Repire all dexfile end!Please enjoy!
```

修复后的 dex 位于当前目录下的 repire 目录，下图为该目录，以及修复的 dex 文件截图。

此电脑 > 桌面 > FART脱壳王定制版自动化修复工具

名称	修改日期	类型	大小
repair	2024/1/11 12:39	文件夹	
test	2024/1/11 12:39	文件夹	

此电脑 > 桌面 > FART脱壳王定制版自动化修复工具 > repair

名称	修改日期	类型
10978168_dexfile.dex_repaired.dex	2024/1/11 12:39	DEX
10978168_dexfile_LoadMethod.dex_repaired.dex	2024/1/11 12:39	DEX
10978168_dexfile_OpenCommon.dex_repaired.dex	2024/1/11 12:39	DEX

修复完成后，只需要使用 jadx、jeb、gda 等打开即可。马上开始你的丝滑逆向之旅吧！

FART脱壳王



长按扫码查看详情